Abstract

The invention relates to a method for exchanging at least one secret initial value between a processing station and a chip card, in an initializing step for the chip card.

In the initialization of chip cards in known methods an initial value, e.g. a key, is transmitted from a processing station to the chip card and stored therein. Since this key is transmitted in plaintext this involves security problems.

In the present invention the described security problems are solved by only parts of the key being exchanged between processing station and chip card and the key being generated in the chip card and the processing station from the parts.